ABSTRACT

A method and system for detecting and removing malicious code from a computer system. The method determines an operating system of the computer system, scans the computer system for malicious code based on the operating system and detects the malicious code. The method and system may also remove the malicious code from the computer system. The method may retrieve from a data file, information relating to the malicious code including at least one command for restoring the computer system to a state that existed prior to modification by the malicious code, and may execute the at least one command for restoring the computer system to substantially the same state as it existed prior to modification by the malicious code. The method scans predetermined memory locations based on the operating system.